UNITED STATES DISTRICT COURT

DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA	)	
	)	
v.	)	CRIMINAL NO. 09-10243-MLW
	)	
RYAN HARRIS	)	

MOTION TO DISMISS INDICTMENT FOR LACK OF VENUE;
ALTERNATIVELY FOR TRANSFER IN THE INTERESTS OF JUSTICE

Defendant, Ryan Harris, respectfully moves this Court, pursuant to Fed. R. Crim. P. 12 and 18, to dismiss the indictment for lack of venue in the District of Massachusetts. Alternatively, Harris moves, pursuant to Fed. R. Crim. P. 21(b), for a transfer to the United States District Court for the Eastern District of California, because such a transfer is in the interest of justice and because the government has disclosed its intention to commence in that District criminal proceedings against defendant for tax offenses relating to this charged conduct.

I. THE INDICTMENT AND THE NATURE OF THE CHARGES[1]

The indictment alleges that Harris lived in California and that he was founder, owner and software developer for defendant TCNISO, a California-based and incorporated developer of "cable modem hacking" software and hardware. Indictment at ¶ 2. The indictment further contends that defendant "knew" that "users"

[1]The following section draws on material received from the government during discovery. Harris recites these facts to orient the Court and does not mean to endorse them as true or correct.

used TCNISO's products to access the internet without paying for some or all of the service. Indictment at ¶ 21. Only one alleged user is identified.

Throughout the indictment, the charges are framed in the language of secondary liability, that Harris aided and abetted, or conspired with, "others" who "used" products to evade service fees. Harris is, essentially, a component manufacturer charged in this venue, distant from his domicile and place of business, with claims of complicity in the theft of service by unnamed "others."

A. The Technology

In order to access the internet through a cable network, a subscriber installs a cable modem, which allows an individual's computer to communicate with an internet service provider ("ISP"). Each modem has an identifier called a media access control (a MAC address). When a cable modem is connected to a cable belonging to an ISP, the modem sends its MAC address to the ISP. If the ISP recognizes that MAC address as belonging to the cable modem of a subscriber, the ISP will allow that modem, and that subscriber, to access the internet. This access will be provided at the speed the customer/owner of the modem has purchased. If the ISP does not recognize the MAC address, it will not allow the modem to access the internet.

According to the government, TCNISO's products and website allowed individuals to shortcut the usual procedures. Allegedly,

one TCNISO product, called Blackcat, was a combination of hardware including a modem and software called Sigma, which enhanced end-users capability, but which the government alleges permitted an individual to change his or her modem's MAC address (also called "spoofing") and thereby receive faster or free internet access. For example, if user A paid for the slowest internet access but used Blackcat to change the MAC address of his or her modem to the MAC address that belonged to user B's modem, and user B received the fastest internet access, the ISP would mistakenly believe that user A was user B, and would provide user A with the fastest internet access. This process is known as modem "uncapping." Allegedly, TCNISO products also allowed ISP subscribers to receive faster service than they purchased by changing the configuration files on their modems. When an individual purchased internet service, the ISP assigned their modem a configuration file that corresponded with the speed of access they have purchased.

The government asserts that Blackcat also enabled TCNISO users to commit outright theft of service by getting internet access for free. According to the government, if a non-customer attached a modem to an unused ISP cable and used Blackcat to change its MAC address to coincide with the MAC address of an ISP subscriber's modem, the ISP would respond as if the non-subscriber was a subscriber and would provide him or her with internet access through the unused cable. The government notes

that this MAC address spoofing allowed people to get free or faster internet access and to mask their identity while they browse the internet.

In addition to products like Blackcat, the government alleges that TCNISO made a product called Coaxthief that allowed individuals to find (or "sniff") the MAC addresses of other individuals' modems. The government asserts that the TCNISO website was a forum that TCNISO users used to trade MAC addresses,[2] and to discuss their experiences and problems with using the products to get faster or free internet.

B. Statutory Framework

Count one of the indictment charges TCNISO and Harris with conspiracy under 18 U.S.C. § 371 to commit computer fraud in violation of 18 U.S.C. §1030(a)(4) and wire fraud in violation of 18 U.S.C. §1343. Count two charges Harris with aiding and abetting computer fraud in violation of 18 U.S.C. §§ 1030(a)(4) and 2. Counts three through six charge Harris with aiding and abetting wire fraud in violation of 18 U.S.C. §§ 1343 and 2.

The computer fraud statute penalizes someone who:

> knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended

[2]Apparently, an individual can only sniff MAC addresses in his or her own area. However, if that individual changed his or her MAC address to coincide with the MAC address of another person in his or her region, the ISP would not allow both individuals to access the internet at the same time. Therefore, people who want to get internet access in this way must find a MAC address from outside their area.

> fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $ 5,000 in any 1-year period.

18 U.S.C. §1030(a)(4).

The government alleges that the unnamed "users" either exceeded their authorized access (by obtaining faster internet access) or accessed the ISP without authorization (obtaining free internet access).

With respect to wire fraud, the government alleges that Harris committed substantive wire fraud by aiding and abetting "others" with the execution of the scheme involving a single person's theft of service. In connection with the allegation of conspiracy to commit wire fraud, it also alleges aiding and abetting "others."

C. Product Users

The indictment identifies a single user and a single affected ISP, but is more broadly framed. In response to a discovery letter dated May 17, 2010, the government claims intrusions into no fewer than 22 internet service providers, and claims that this number may increase as investigation continues. The government asserts that the dates of user access were too many to detail: "Because many of the TCNISO customers who used the company's products to access ISPs' networks without authorization did so on a regular basis, we cannot identify the dates of all of these accesses." Discovery Letter, May 17, 2010.

Indeed, except for the single named user, the government has provided no identifying details regarding "users" and their alleged activities. It bears noting that the word "user" was employed to signify all who acquired TCNISO products, even non-customers.

D. Allegations Specific to Massachusetts

The indictment alleges two links to this District. The first relates to the single identified "user," a Massachusetts resident named DShocker, who allegedly used products developed by TCNISO to access the internet without paying.[3] DShocker allegedly also used the TCNISO forums to get advice and MAC addresses and to talk about his use of the free internet service, including communicating online with Harris and other unindicted coconspirators "about cable modem hacking." Id. at ¶ 30.[4] The indictment implies that DShocker performed all of these activities in the state of Massachusetts.

[3]The government has orally indicated that it knows of other TCNISO users who live in Massachusetts. These sales are not mentioned in the indictment, and counsel has not received any information identifying these individuals or any details about them or their actions.

[4]Discovery materials call into question which products DShocker received and from whom. His Grand Jury testimony indicates that he initially got a modem that he planned to use to get free internet access "from somebody on another website." Grand Jury Testimony, May 6, 2009, Bates Harris208. He also testified that some of the software he used to gain free internet access did not come "directly from TCN[ISO], but it was from somebody who had gotten it from TCN[ISO]." Id. at Harris221.

The second alleged link was government-generated. In late 2008, an FBI agent in Boston, Massachusetts accessed the TCNISO website and bought five modems and a copy of Hacking the Cable Modem, a book authored by defendant. To complete this purchase, the agent called TCNISO in California, and spoke with someone named "Ryan." The agent subsequently received the modems and book in Massachusetts. According to the indictment, "[t]hese modems were capable of hacking a cable network and obtaining free internet service." Id. at ¶ 39.

Apart from DShocker and the FBI agent, none of the entities and individuals mentioned in the indictment reside in or are alleged to have entered Massachusetts at any time. According to the indictment, unindicted co-conspirator one, a software developer for TCNISO, resided in Kentucky; and unindicted co-conspirator two, the former vice-president of TCNISO, lived in California. None of these individuals is alleged to have entered or to have specifically sought contact with anyone in Massachusetts.

ARGUMENT

I. Venue is not Proper in this District

The government does not charge that TCNISO's products as designed violated federal law, nor would venue have existed in this District for such a claim. Instead, the government asserts that the products as used violated federal law, that defendant knew that downstream users "used TCNISO's products to gain

unauthorized access to various ISPs' networks..." Indictment at ¶ 21.

Alleging secondary liability to bootstrap venue in this District poses its own venue problems. Secondary liability presumes primary culpability, raising particularized questions: with whom, when and how? Particulars of this sort are the stuff of separate counts of an indictment, not of a single duplicitous pleading. Moreover, an individual user of a computer component is not, without more, complicit in a conspiracy with the product manufacturer, particularly when the "user" was not a customer. Only the existence of some complicitous "more" might create conspiratorial culpability with the seller, but that is a fact-specific inquiry and a particularized conspiratorial agreement.

As is more fully set forth below, efforts to charge secondary conduct as a venue device fail.

A. Venue Generally

When a defendant challenges the government's choice of venue, "the government must prove by a preponderance of the evidence that venue is proper as to each individual count." United States v. Salinas, 373 F.3d 161, 163 (1st Cir. 2004). Generally, venue is proper if the district of the trial is a district in which the crime charged occurred.

The constitutional limits on venue in criminal cases derive from two provisions of the Constitution and from the Federal Rules of Criminal Procedure. See United States v. Cabrales, 524

U.S. 1, 6 (1998) (delineating law governing choice of venue); Salinas, 373 F.3d at 164 ("The importance of [the defendant's right to be tried in an appropriate venue] is emphasized by the fact that it is mentioned not once, but twice, in the text of the Constitution."). Article III requires that criminal trials "shall be held in the State where the said Crimes shall have been committed." U.S. Const. art. III, § 2, cl. 3. The Sixth Amendment further specifies that "[i]n all criminal prosecutions, the accused shall enjoy the right to a speedy and public trial, by an impartial jury of the State and district wherein the crime shall have been committed." U.S. Const. amend. 6. Rule 18 of the Federal Rules of Criminal Procedure codifies the constitutional command, stating that "the government must prosecute an offense in a district where the offense was committed." Fed.R.Crim.Pro. 18. The First Circuit has stated that it is "apparent that venue requirements promote both fairness and confidence in the criminal justice system." Salinas, 373 F.3d at 164.

The federal courts have explained that the "'locus delicti must be determined from the nature of the crime alleged and the location of the act or acts constituting it.'" Salinas, 373 F.3d at 164 (quoting United States v. Anderson, 328 U.S. 699, 703 (1946)). Although the action verbs contained in the statute should not be the sole consideration in determining where a crime occurred, a court's consideration of venue "must begin by 'identify[ing] the conduct constituting the offense (the nature

of the crime) and then discern the location of the commission of the criminal acts.'" Id. (quoting United States v. Rodriguez-Moreno, 52 U.S. 285, 279 (1999)).

B. Venue Is Not Proper in Massachusetts

To claim venue in this District, resting on the alleged actions of a single Massachusetts user, the government alleges (a) that a seller of a product conspires with, and aids and abets, his users, and (b) that actions of one user can be linked into a common count joining all users.

a. A User of a Computer Component is not an Aider and Abettor or a Conspirator with the Seller

In United States v. Peoni, the defendant sold counterfeit currency to another party who sold it to a third party. 100 F.2d 401, 401-02 (2nd Cir. 1938). The court ruled that Peoni could not be an accomplice to or in conspiracy with the third party's crime of possession. Id. at 402-03. In his opinion, Judge Learned Hand noted the difference between the scope of criminal and civil liability.

> The prosecution's argument is that, as Peoni put the bills in circulation and knew that Regno would be likely, not to pass them himself, but to sell them to another guilty possessor, the possession of the second buyer was a natural consequence of Peoni's original act, with which he might be charged. If this were a civil case, that would be true; an innocent buyer from Dorsey could sue Peoni and get judgment against him for his loss. But the rule of criminal liability is not the same; since Dorsey's possession was not de facto Peoni's, and since Dorsey was not Peoni's agent, Peoni can be liable only as an accessory to Dorsey's act of possession.

Id. at 402. Judge Hand went on to explain that criminal liability for an accessory only applies when the accessory "in some sort associate himself with the venture, that he participate in it as in something that he wishes to bring about, that he seek by his action to make it succeed." Id.; see also United States v. Medina-Roman, 376 F.3d 1, 3 (1st Cir. 2004) ("The roots of modern doctrines of aiding and abetting liability can be traced to Judge Learned Hand's famous formulation in [Peoni]."), cert. denied 543 U.S. 993.

These limits on criminal liability are examined in cases similar to the one at hand. In a case involving defendants accused of selling modules that could modify cable converter boxes in order to get free cable television service, the Seventh Circuit noted that a "mere buyer-seller relationship" is not a criminal conspiracy. United States v. Gee, 226 F.3d 885, 895 (7th Cir. 2000). Similarly, it is not enough for the government to show that Harris sold legal goods knowing that the goods would be used for illicit ends by the users; the government must show that Harris knew about and intended to join a conspiracy. See United States v. Falcone, 311 U.S. 205, 208-10 (1940) (holding that seller's knowledge that legal goods would be used in illicit distilling did not support a conspiracy conviction where seller did not know of or agree to join distilling conspiracy); Direct Sales Co. v. United States, 319 U.S. 703, 709 (1943) ("[O]ne does

not become a party to a conspiracy by aiding and abetting it, through sales of supplies or otherwise, unless he knows of the conspiracy; and the inference of such knowledge cannot be drawn merely from knowledge the buyer will use the goods illegally.").

The government's pleading, with its broad ranging accusations of complicity with "others," abandons these well-developed legal doctrines. Its approach more closely mimics the civil notion of contributory liability than any theory of criminal liability. Illustrative is MGM Studios, Inc. v. Grokster, 545 U.S. 913 (2005), where copyright holders sued Grokster alleging that Grokster's software was intended to allow users to download copyrighted works. The Supreme Court endorsed the availability of theories of contributory and vicarious liability to permit indirect civil liability, noting that "[w]hen a widely shared service or product is used to commit infringement, it may be impossible to enforce rights in the protected work effectively against all direct infringers, the only practical alternative being to go against the distributor of the copying device for secondary liability on a theory of contributory or vicarious infringement." Id. at 929-30. Akin to the Grokster approach, the government here foregoes suit against direct cable trespassers in favor of proceeding against defendant. But it eviscerates long-honored legal boundaries by recasting as criminal a civil legal theory. It does so, transparently, to engineer venue in this District, as if the

criminal law countenances such a stratagem. To invoke and paraphrase Judge Hand: "the rule of criminal liability is not the same [as civil]"; if this were a civil case, an innocent ISP might seek to recover (or enjoin) defendant and defendant company, but since a user's conduct is not de facto defendant's, and the users were not defendant's agent, defendant is not liable, absent more, for the manner of use by "others."

B. The Device of a Duplicitous Charge Does Not Create Venue

The indictment alleges that defendant knew that a single named Massachusetts resident was using TCNISO software and hardware to trespass onto the network of a single ISP. It then links, within the single substantive count of computer fraud, alleged acts of "others" in computer trespasses. To aid and abet defendant must have specific knowledge or have actually aided "others" in their theft of service.

"Duplicity is the joining in a single count of two or more distinct and separate offenses." United States v. Verrecchia, 196 F.3d 294, 297 (1st Cir. 1999) (quoting United States v. Martinez Canas, 595 F.2d 73, 78 (1st Cir. 1979)); see also Fed. R.Crim.P. 8(a). Duplicitous indictments are prohibited in part because a jury could convict an individual without having agreed unanimously that the individual committed any one particular act. Id. A duplicitous indictment may also "(1) fail to give the defendant adequate notice of the nature of the charges,

(2) threaten to subject the defendant to prejudicial evidentiary rulings at trial, and (3) produce trial records inadequate to allow a defendant to plead prior convictions or acquittals as a bar to subsequent prosecution for the same offense." United States v. D'Amico, 496 F.3d 95, 99 n.3 (1st Cir. 2007) (vacated for reconsideration under Gall v. United States, 552 U.S. 38 (2007) by D'Amico v. United States, 552 U.S. 1173 (2008)). One might add that the government might charge duplicitously to aid a claim to venue.

Here, a single charge aggregates an unspecified number of alleged trespasses by actors yet unknown into more than 22 protected computers. Unlike the usual approach to secondary liability, where an aider and abetter is alleged to further the conduct of a specific primary actor, the government's theory is that it may charge secondary conduct premised on product capability in the hands of unknown "others," together with defendant's knowledge and intent regarding that capability. But each computer trespass is separate, dependent on proof of the software/hardware used, the manner of the access to the respective "protected computer," and any alleged involvement by defendant with that intrusion. Violations of the Computer Fraud Act also require proof of the underlying crime that the "access" was in furtherance of, accusations presumably singular for each alleged trespasser. Cumulating multiple, perhaps even hundreds of separate alleged trespasses into a single count, makes the

charge "duplicitous" because it charges distinct offenses in a single count. The duplicitousness of the charges is not alleviated in the conspiracy count. As explained above, a mere buyer-seller relationship is not necessarily a conspiracy. See, e.g., Gee, 226 F.3d at 895.

c. The Remaining Contacts with this District do not Support Venue

The purchase of modems and a book, undertaken by an undercover agent who was located in Massachusetts, does not confer venue. An investigating agent's phone call to a target, made from a location of the agent's choosing and on the eve of prosecution, is not a meaningful measure of the locus of a crime. It is instead an invitation to manipulate the venue of an action. TCNISO's actions were all taken in California, and no representative of the company is alleged to have come to or initiated contact with anyone in Massachusetts. Allowing this transaction to serve as the basis for venue would allow the government to manufacture venue in any district in the country. See United States v. Naranjo, 14 F.3d 145, 147 (2nd Cir. 1994) (rejecting defendant's argument that the government had "artificially created venue," but implying that a trial is not proper in a district where the government had "orchestrated" venue), cert. denied, 511 U.S. 1095. Permitting the government to create venue in this way would nullify the constitutional limits on venue.

The government also alleges that DShocker's activities make venue proper in Massachusetts. As with the shipment to the FBI agent, there is no allegation that Harris went to Massachusetts, that he sought contact with DShocker in Massachusetts, or that he knew where DShocker lived. In fact, documents received in discovery indicate that DShocker never told anyone his real name or where he lived. FBI Interview Notes Sept. 16, 2008 at 3, Bates Harris1632. Additionally, it is clear from discovery materials that there is a serious question as to what items DShocker got from Harris and TCNISO, and what he got from other individuals. DShocker testified in the Grand Jury that he initially got a modem that he planned to use to get free internet access "from somebody on another website." Grand Jury Testimony, May 6, 2009, Bates Harris208. At the same time, he testified that some of the software he used to gain free internet access did not come "directly from TCN[ISO], but it was from somebody who had gotten it from TCN[ISO]." Id. at Harris221. An individual who sells a product to someone who then sells that product to a third party, cannot be criminally liable for the actions of that third party. See Peoni, 100 F.2d at 402.

Because the government cannot establish that venue is proper by a preponderance of the evidence, this court should dismiss the indictment for lack of venue.

II. Venue Should be Transferred for the Convenience of the Parties and in the Interest of Justice

Alternatively, Harris asks this court to transfer venue to the United States District Court for the District of Eastern District of California, because adjudicating this matter in this district would be a substantial burden. The Federal Rules of Criminal Procedure provide that: "Upon the defendant's motion, the court may transfer the proceeding, or one or more counts, against that defendant to another district for the convenience of the parties and witnesses and in the interest of justice." Fed. R.Crim.P. 21(b).

Rule 21(b) gives a district court "broad discretionary power to transfer a criminal prosecution to another district." United States v. Muratoski, 413 F.Supp.2d 8, 9 (D.N.H. 2005). The Supreme Court and district courts in the First Circuit have identified ten factors that a judge considering a motion under Rule 21(b) should consider: (1) the location of the defendant; (2) the location of possible witnesses; (3) the location of events likely to be in issue; (4) the location of documents and records likely to be involved; (5) the disruption of defendant's business if the case is not transferred; (6) the expense to the parties; (7) the location of counsel; (8) the relative accessibility of the place of trial; (9) the docket condition of each district or division involved; and

(10) any other special considerations relevant to transfer. See id.

First, Harris and his family live in Oregon. It is a hardship for him to face trial on the opposite side of the country. Second, the potential witnesses who are likely to be in Massachusetts are DShocker and any FBI agents who were involved in the case in Massachusetts. However, there are at least an equal number of potential witnesses who are located on the West Coast, for example, unindicted co-conspirator one is alleged to live in California, TCNISO store employees are likely in California, and there were FBI agents involved in the case in California, including those who watched, visited, and searched the TCNISO store. Third, as discussed above, the crux of activity that will be at issue in this trial occurred in California. The overt acts that are alleged to have occurred in Massachusetts either involve DShocker or the elective acts of the government in accessing a website and ordering materials to be sent to Massachusetts. Many of the most highly contested aspects of this trial involve Harris's conduct and knowledge, and all of his actions are alleged to be California-based. Fourth, because TCNISO was based in California, it is likely that any documents not easily accessible in an electronic form are located there. Fifth, facing trial on the East Coast would significantly disrupt Harris's life and his ability to work. Sixth, facing trial

across the country would impose a major emotional and financial toll on Harris and his family. Seventh, appointed counsel is available in California. Eighth, a trial in the Eastern District of California would be significantly more convenient for Harris, while moving the trial there is not likely to inconvenience the government. Ninth, statistics available on the United States Courts website show that since 2009, the number of criminal filings in the Eastern District of California has decreased and the number of case terminations has increased. U.S. Courts, Federal Judicial Caseload Statistics, available at http://www.uscourts.gov/Viewer.aspx?doc=/uscourts/Statistics/FederalJudicialCaseloadStatistics/2010/tables/D00CMar10.pdf (last visited Jan. 21, 2011). The District of Massachusetts has seen the same changes, indicating that docket conditions should not impede this transfer.

Finally, a major factor in favor of a discretionary transfer is the fact that the government has stated that it intends to file a case charging Harris with tax fraud in the Eastern District of California. The charges relate directly to TCNISO, and its revenues, and any tax obligations defendant may have had as a result, and implicate some of the same discovery. If this case remains in this District, defendant will have to simultaneously defend himself against tax charges in the Eastern District of California. He will

have to consult with two lawyers and to deal with two courts regarding the same time and actions.

For all of these reasons, Harris asks this Court to transfer venue to the Eastern District of California for the convenience of the parties and in the interest of justice.

III. CONCLUSION

This Court should dismiss the indictment against Harris for lack of venue. The government cannot establish, by a preponderance of the evidence, that venue is therefore proper in the District of Massachusetts. In the alternative, this Court should transfer the case to the Eastern District of California in the interests of justice.

RYAN HARRIS
By his attorney,

/s/ Charles P. McGinty

Charles P. McGinty
B.B.O. #333480
Federal Defender Office
51 Sleeper Street
Boston, MA 02210
Tel: 617-223-8061

CERTIFICATE OF SERVICE

I hereby certify that this document, filed through the ECF system, will be sent electronically to the registered participants as identified on the Notice of Electronic Filing (NEF) and paper copies will be sent to those indicated as non-registered participants on January 24, 2011.

/s/ Charles P. McGinty

Charles P. McGinty